Quantum Computing

Alessandra Di Pierro

1 Esercitazione 4

Esercizio 1.1 *Trovare l'espansione in frazioni continue di 37/17.*

Esercizio 1.2 *Calcolare MCD(231,315) con l'algoritmo di Euclide.*

Esercizio 1.3 (Fattorizzazione mediante l'algoritmo di Shor) *Illustriamo l'esecuzione dell'algoritmo quantistico per la fattorizzazione descritto a lezione, applicandolo per trovare i fattori di* $N = 15$.

Passo 1 Supponiamo di scegliere il numero casuale $x = 7$.

Passo 2 Con l'algoritmo di Euclide otteniamo $MCD(7, 15) = 1$. Quindi procediamo con il passo 3.

Passo 3 Calcoliamo l'ordine di 7 modulo 15 usando l'algoritmo quantistico studiato a lezione.

- Fissiamo $\epsilon = 1/4$ e $n = 2L + 1 = 2 \cdot 4 + 1 = 9$, ottenendo $t = 2L + 1 + \log 2 + 1/2\epsilon = 9 + \log 4 = 11$.
- Prepariamo il primo registro nello stato $|0\rangle^{\otimes t}$ e il secondo registro nello stato $|1\rangle$, ottenendo lo stato iniziale $|\psi_0\rangle = |0\rangle\,|1\rangle$.
- Applichiamo la trasformata di Hadamard al primo registro ottenendo

$$|\psi_1\rangle = \frac{1}{\sqrt{2048}} \sum_{k=0}^{2047} |k\rangle\,|1\rangle$$

- Applichiamo la sequenza di operazioni controlled-U, dove $U\,|y\rangle = |7y(mod15)\rangle$ a $|\psi_1\rangle$, ottenendo

$$|\psi_2\rangle \quad = \quad \frac{1}{\sqrt{2048}} \sum_{k=0}^{2047} |k\rangle \left|7^k (mod15)\right\rangle$$

$$= \frac{1}{\sqrt{2048}} [|0\rangle |1\rangle + |1\rangle |7\rangle + |2\rangle |4\rangle + |3\rangle |13\rangle +$$
$$= + |4\rangle |1\rangle + |5\rangle |7\rangle + |6\rangle |4\rangle + \dots] .$$

- Applichiamo la trasformata di Fourier inversa $FT^\dagger$ al primo registro e misuriamolo per ottenere φ. Un modo per analizzare la distribuzione dei risultati ottenuti é quello di applicare il principio della misurazione implicita, secondo il quale ogni qubit che al termine di un circuito non é stato misurato si puó assumere come terminato da un'operazione di misurazione. Nel nostro caso, poiché sul secondo registro non verranno applicate ulteriori operazioni, possiamo assumere che il secondo registro venga misurato ottenendo un risultato random tra 1, 7, 4 e 13 (Notare la periodicitá della funzione $x^k (mod N)$. Supponiamo di ottenere 4. Allora lo stato del primo registro collassa a

$$\frac{1}{\sqrt{2048/4}} [|2\rangle + |6\rangle + |10\rangle + |14\rangle + \dots] .$$

  A questo stato viene applicata la $FT^\dagger$ risultando in un certo stato $\sum_l \alpha_l |l\rangle$. Analizzando la distribuzione di probabilitá dei risulati sull'intervallo da 0 a 2048 ottenuti dalla misurazione finale, si vede che i risultati con la probabilitá piú alta (e molto vicina a 1/4) corrispondono a 0, 512, 1024 o 1536. Supponiamo di ottenere il risultato 1536. Allora otteniamo $\varphi = 1536/2048$.

- Calcoliamo l'espansione in frazioni continue di φ: $1536/2048 = 1/(1 + (1/3))$, da cui risulta che 3/4 é un convergente di φ. Verifichiamo quindi che $r = 4$ é effettivamente l'ordine di 7 modulo 15.

Passo 4 r é pari e $7^2 = 4 (mod 15) \neq -1 (mod 15)$. Quindi possiamo proseguire con il passo successivo.

Passo 5 Calcoliamo infine i massimi comun divisori $MCD(x^2 - 1, 15) = 3$ e $MCD(x^2 + 1, 15) = 5$, e concludiamo che sono due fattori non banali di 15.

Esercizio 1.4 *Applica l'algoritmo di Shor per fattorizzare* 15 *con con l'assunzione che si scelga* $x = 13$ *al* **Passo 1**. *Ripetere per* $N = 91$ *e* $x = 4$ *e per* $N = 18$ *con* $x = 5$.

Esercizio 1.5 *Applica l'algoritmo di Shor per fattorizzare l'intero* 21. *Fornisci due esecuzioni dell'algoritmo di cui una ha successo e l'altra fallisce.*

Esercizio 1.6 *Considera la funzione definita da*

$$f(k) = x^k (mod N),$$

dove x e N sono interi positivi. Dimostra che f é periodica sotto un'opportuna ipotesi e descrivi un algoritmo quantistico polinomiale per trovare il periodo della funzione f.